



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



Cyberbezpieczny  
Samorząd

## 1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu zewnętrznego w Urzędzie Miasta i Gminy w Sycowie oraz Centrum Usług Społecznych w Sycowie w zakresie:

1. Zgodności z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI)
2. Zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC)

**w zakresie obowiązków nałożonych na oba podmioty publiczne**

---

## 2. Zakres prac

### Część I: Audyt KRI (Zarządzanie Bezpieczeństwem Informacji)

Audytory musi zweryfikować, czy obie jednostki posiadają i stosują System Zarządzania Bezpieczeństwem Informacji (SZBI), w tym:

- **Analiza ryzyka:** Ocena metodyki oraz aktualności przeprowadzonej analizy ryzyka dla zasobów informacyjnych.
- **Polityki i procedury:** Przegląd dokumentacji (Polityka Bezpieczeństwa Informacji, Instrukcja Zarządzania Systemami Informatycznymi).
- **Zarządzanie uprawnieniami:** Kontrola procesów nadawania, odbierania i przeglądu dostępów do systemów.
- **Ciągłość działania:** Weryfikacja planów awaryjnych oraz procedur tworzenia i testowania kopii zapasowych (backup).
- **Szkolenia:** Ocena realizacji szkoleń z zakresu bezpieczeństwa informacji dla pracowników.

### Część II: Audyt UKSC (Cyberbezpieczeństwo)

Weryfikacja wypełniania obowiązków ustawowych, w tym:

- **Obsługa incydentów:** Sprawdzenie procedur zgłaszania i zarządzania incydentami w systemach informatycznych.
- **Współpraca z CSIRT:** Weryfikacja kanałów komunikacji z właściwym CSIRT (np. CSIRT NASK).
- **Zarządzanie aktywami:** Ocena kompletności inwentaryzacji systemów i sprzętu biorących udział w świadczeniu usług publicznych.



---

### 3. Metodyka i wymagania techniczne

Wykonawca zobowiązany jest do przeprowadzenia audytu z wykorzystaniem min. min następujących metod:

- **Przegląd dokumentacji:** Analiza wewnętrznych regulaminów i zarządzeń.
- **Wywiady:** Rozmowy z kadrą zarządzającą, pracownikami IT oraz Inspektorem Ochrony Danych (IOD).
- **Wizja lokalna:** Sprawdzenie fizycznych zabezpieczeń (serwerownia, dostęp do biur, polityka czystego biurka).

---

### 4. Produkty końcowe

Po zakończeniu prac Wykonawca dostarczy zamawiającemu

- **Raport z audytu:** Szczegółowy opis stanu faktycznego, stwierdzonych uchybień oraz ryzyk.
- **Plan naprawczy:** Konkretnie rekomendacje (techniczne i organizacyjne) mające na celu usunięcie niezgodności.
- **Certyfikat/Poświadczenie:** Dokument potwierdzający przeprowadzenie audytu zgodnie z wymogami prawa.

---

### 5. Wymagania wobec audytorów

Zgodnie z przepisami, audyt musi przeprowadzić osoba posiadająca odpowiednie kompetencje, w tym posiadać co najmniej jeden z certyfikatów:

- **CISA** (Certified Information Systems Auditor)
- **CISM** (Certified Information Security Manager)
- **ISO/IEC 27001 Lead Auditor**
- **CISSP** (Certified Information Systems Security Professional)

---

### 6. Harmonogram i poufność

- **Termin realizacji:** 21 dni od daty podpisania umowy.
- **Poufność:** Wykonawca zobowiązany jest do podpisania Umowy o Zachowaniu Poufności (NDA) przed przystąpieniem do prac.